vision

# Cyber Security Awareness

## Wyoming Office of the CIO

# State IT Security Policy 141

Information Security Awareness and Training

- This policy establishes the requirement for information technology (IT) security awareness and training in all executive branch agencies.
- Security Awareness.  All State employees shall be exposed to security awareness materials throughout the year.
- Recurring Training.  All State employees shall receive an annual refresher that reinforces relevant information security issues.

***http://cio.state.wy.us/standards/srce/web/default.htm***

# Don’t Be a Billy

- http://www.youtube.com/watch?v=nPR131wMKEo

# Anti-virus & anti-malware

- Easy to install, use and update
- Intuitive console
- By default provides:
  - Real-time scanning
  - Email scanning
  - Download scanning
  - Archive scanning
  - Heuristic scanning

# Anti-virus & anti-malware

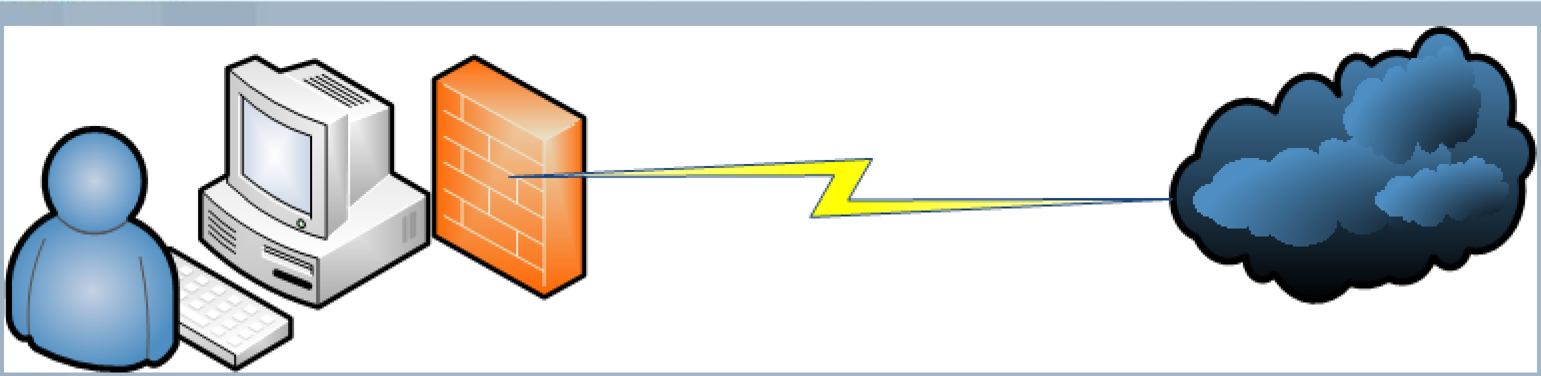
- Avast Home Edition
- AVG Free
- AntiVir Personal
- Microsoft Security Essentials
- SpyBot Search & Destroy
- CCleaner

# Spam filters

- Generally provided by ISP
- Gmail, Hotmail, Yahoo
- “Junk Mail” settings

If you do not know or cannot identify the sender of the email, delete it OR send it to your “junk” folder

# Host-based firewall (HBFW)



Allow or Deny

Protocol (ip, tcp, udp, icmp)

IP address or network

Port (80, 443, 445, 3389)

Application (IE, Firefox, Outlook)

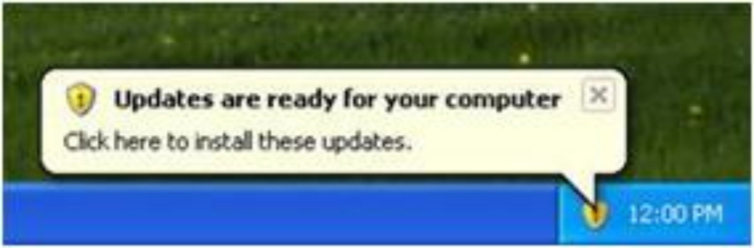
# Host-based firewall (HBFW)

- Windows XP – decent
- Windows Vista & 7 – good
- Zone Alarm
- Outpost
- iptables / ipchains

Why have a firewall if you’re going to allow exceptions?

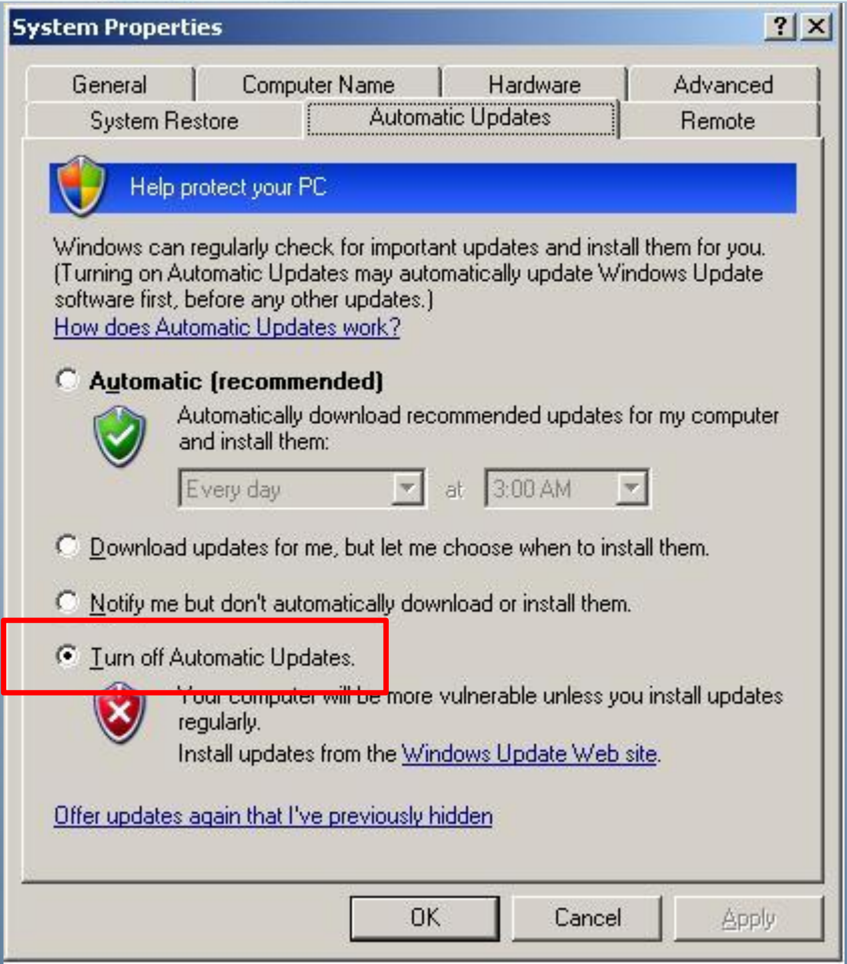
If you don’t need it, block it!!

# Updates



**Updates are ready for your computer**

Click here to install these updates.



**System Properties**

Help protect your PC

Windows can regularly check for important updates and install them for you. (Turning on Automatic Updates may automatically update Windows Update software first, before any other updates.)

How does Automatic Updates work?

○ **Automatic (recommended)**

Automatically download recommended updates for my computer and install them:

Every day at 3:00 AM

○ Download updates for me, but let me choose when to install them.

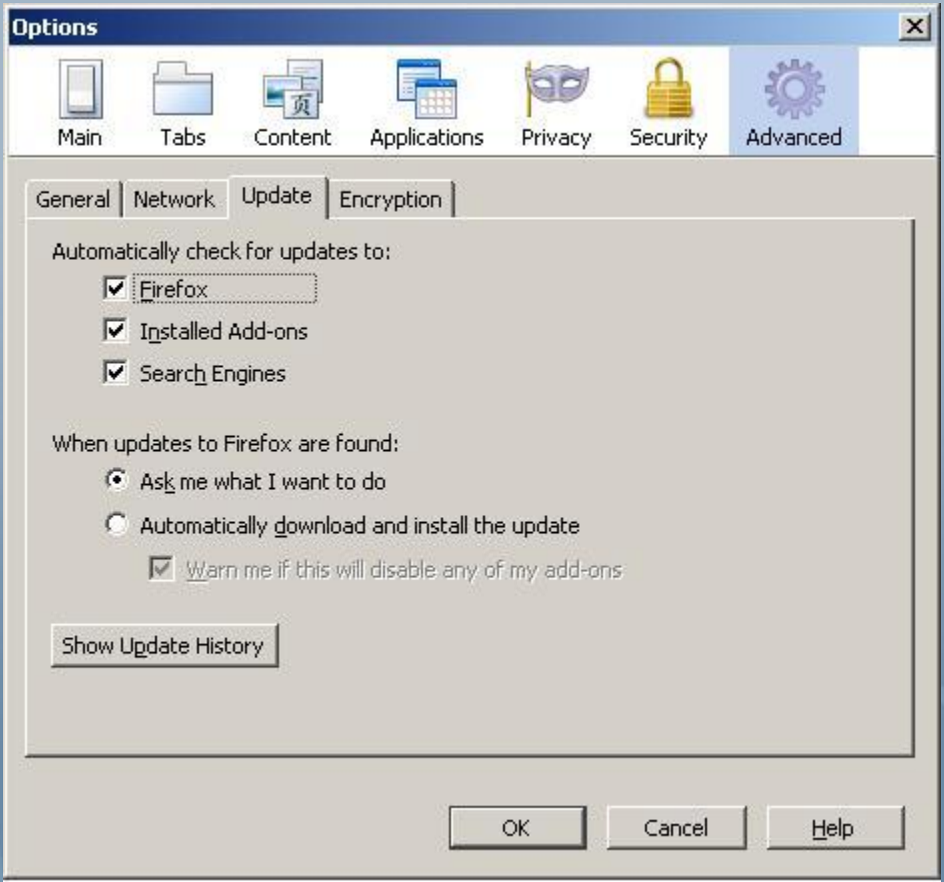
○ Notify me but don't automatically download or install them.

● Turn off Automatic Updates.

Your computer will be more vulnerable unless you install updates regularly.

Install updates from the Windows Update Web site.

Offer updates again that I've previously hidden



**Options**

Automatically check for updates to:

☑ Firefox

☑ Installed Add-ons

☑ Search Engines

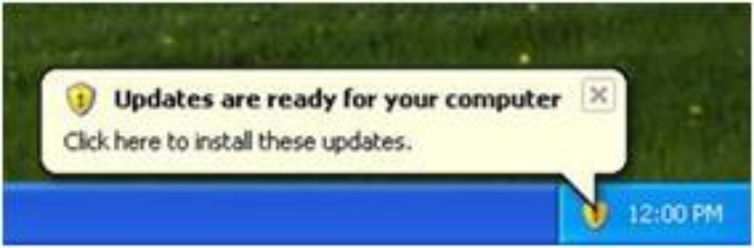
When updates to Firefox are found:

● Ask me what I want to do

○ Automatically download and install the update

☑ Warn me if this will disable any of my add-ons

# Updates



Updates are ready for your computer

Click here to install these updates.

12:00 PM

- At a minimum, check for updates once a month; weekly is better; automatic is preferred
- If technically savvy, use “custom” install to pick updates.
- Tools like Secunia PSI can identify out-of-date applications, plug-ins, and add-ons

# Passwords

- Alpha-numeric, special characters
- 7-12 characters long (or more)
- Change every 60 days or sooner
- Don’t recycle passwords to often
- Different account; different password
- Use a password manager/safe

# Passwords

- 09Rockie$
- 1337 $kilz
- !P@s$W0rD
- 1234567890
- 1Q2W3E4R
- z!x@c#v$
- ???????

Took 10 minutes to crack these passwords

# Passwords

- M3t@b0l!sm
- §3cReT$

mary had a little lamb, its fleece was white as snow

- mhallifwwas
- MhA1l!fwW@s

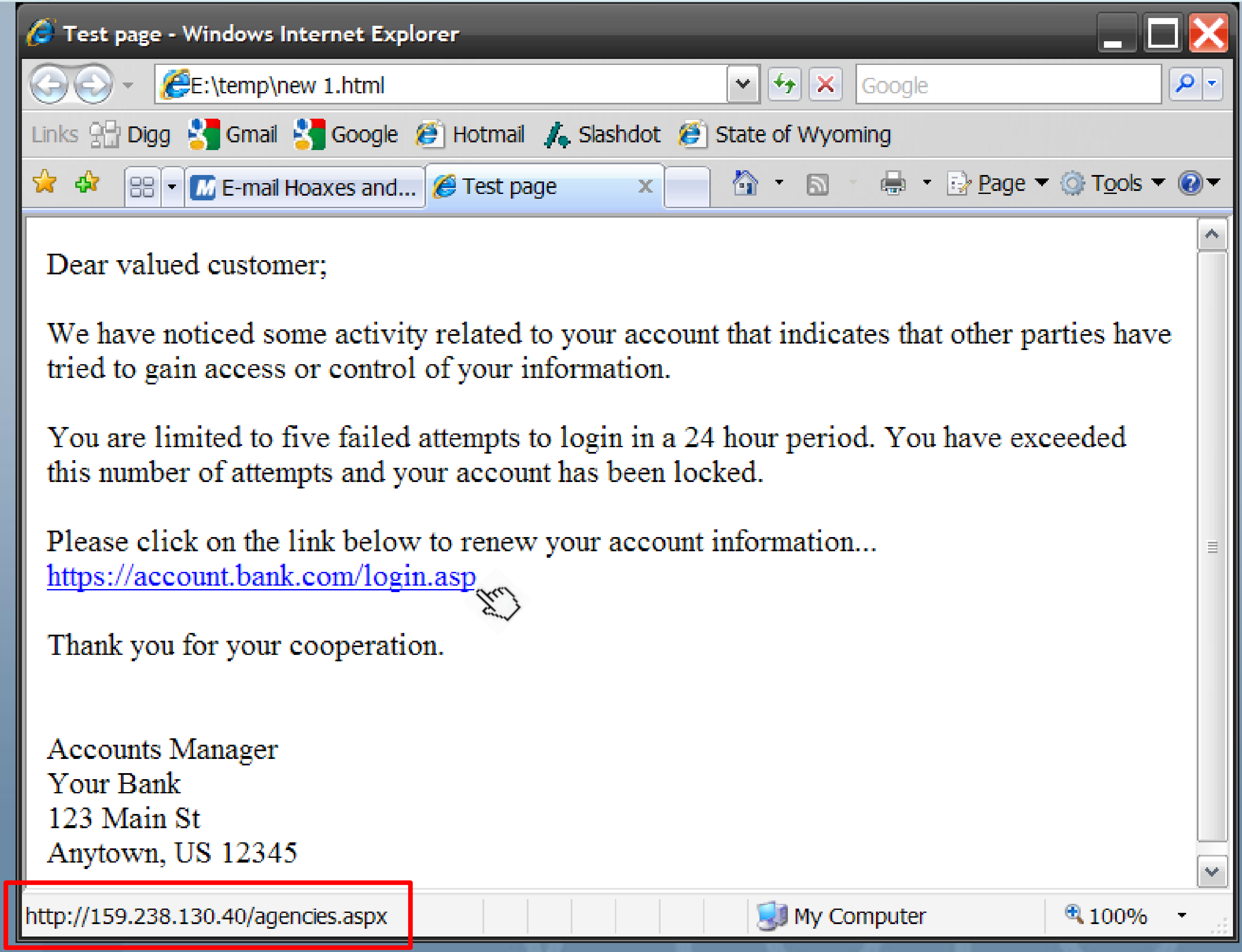
# Personal data

- Would you walk up to a complete stranger and tell them:
  - Bank account info
  - SSN / mothers maiden name
  - Credit card numbers
  - Email address
  - Phone number
  - Home address
- Then rethink posting this online

# Suspicious emails

- Appear to come from your bank or someone you know
- Might ask you to make a phone call
- Might include official looking logos
- Phrases to watch out for:
  - Verify your account
  - You have won the lottery
  - If you don’t respond within 48 hours, your account will be closed

# Suspicious links



Dear valued customer;

We have noticed some activity related to your account that indicates that other parties have tried to gain access or control of your information.

You are limited to five failed attempts to login in a 24 hour period. You have exceeded this number of attempts and your account has been locked.

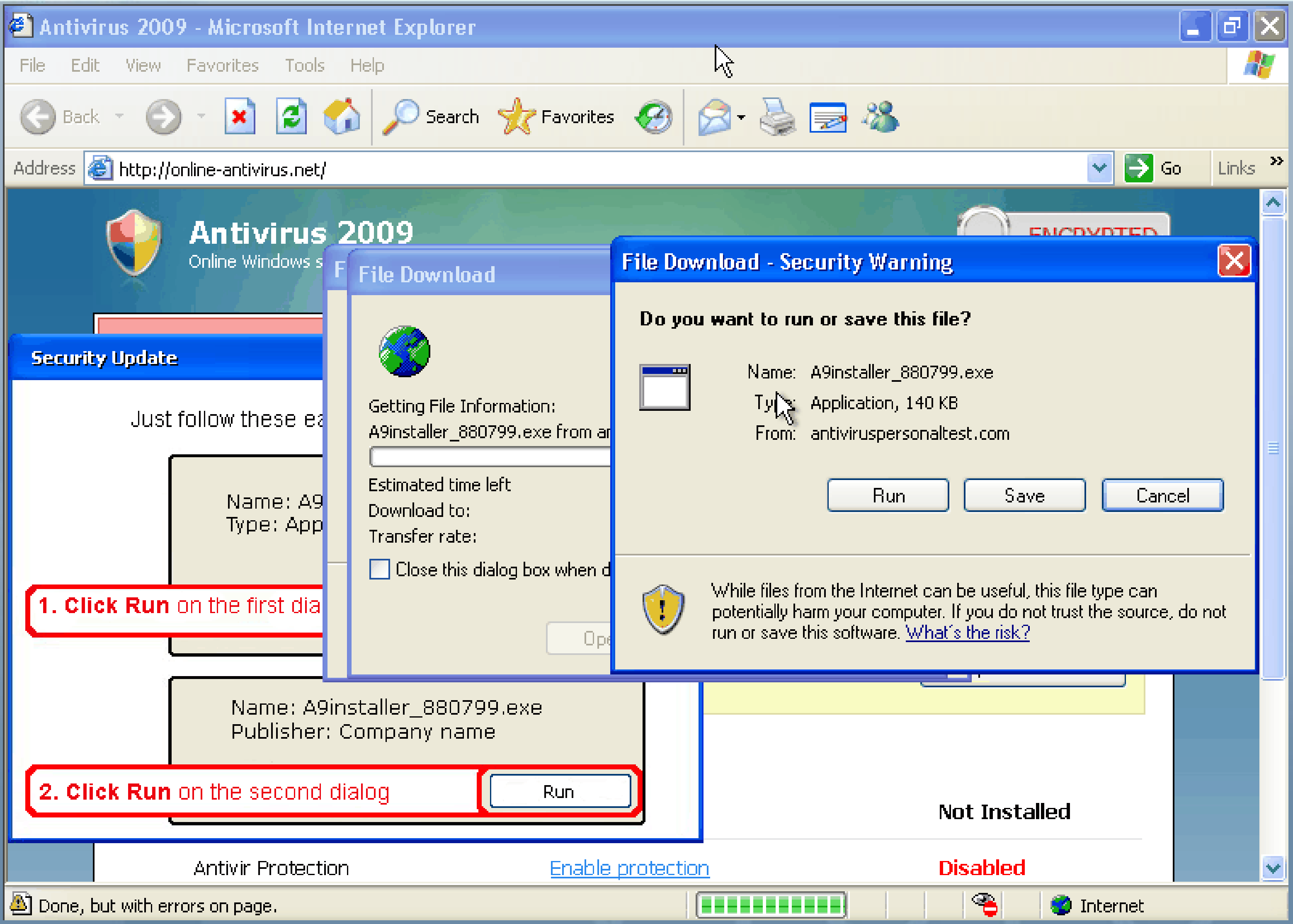
Please click on the link below to renew your account information...
https://account.bank.com/login.asp

Thank you for your cooperation.

Accounts Manager
Your Bank
123 Main St
Anytown, US 12345

http://159.238.130.40/agencies.aspx

# Suspicious links



Antivirus 2009 - Microsoft Internet Explorer

http://online-antivirus.net/

Antivirus 2009

Online Windows s

ENCRYPTED

Security Update

Just follow these ea

Name: A9
Type: App

1. Click Run on the first dia

Name: A9installer_880799.exe
Publisher: Company name

2. Click Run on the second dialog

File Download

Getting File Information:
A9installer_880799.exe from ar

Estimated time left
Download to:
Transfer rate:

□ Close this dialog box when d

File Download - Security Warning

Do you want to run or save this file?

Name: A9installer_880799.exe
Type: Application, 140 KB
From: antiviruspersonaltest.com

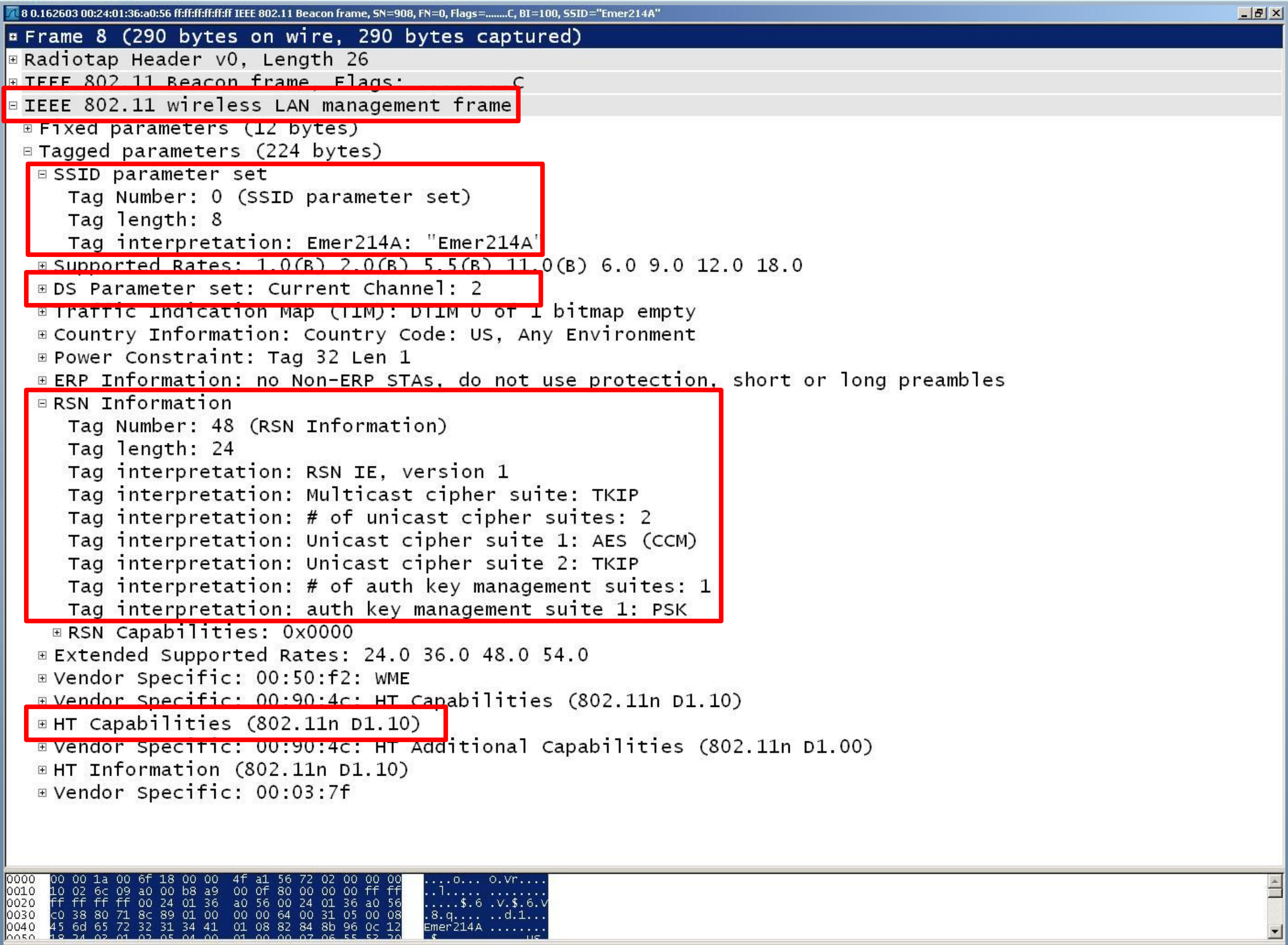
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

Not Installed

Antivir Protection Enable protection Disabled

Done, but with errors on page.

# Encrypted wireless

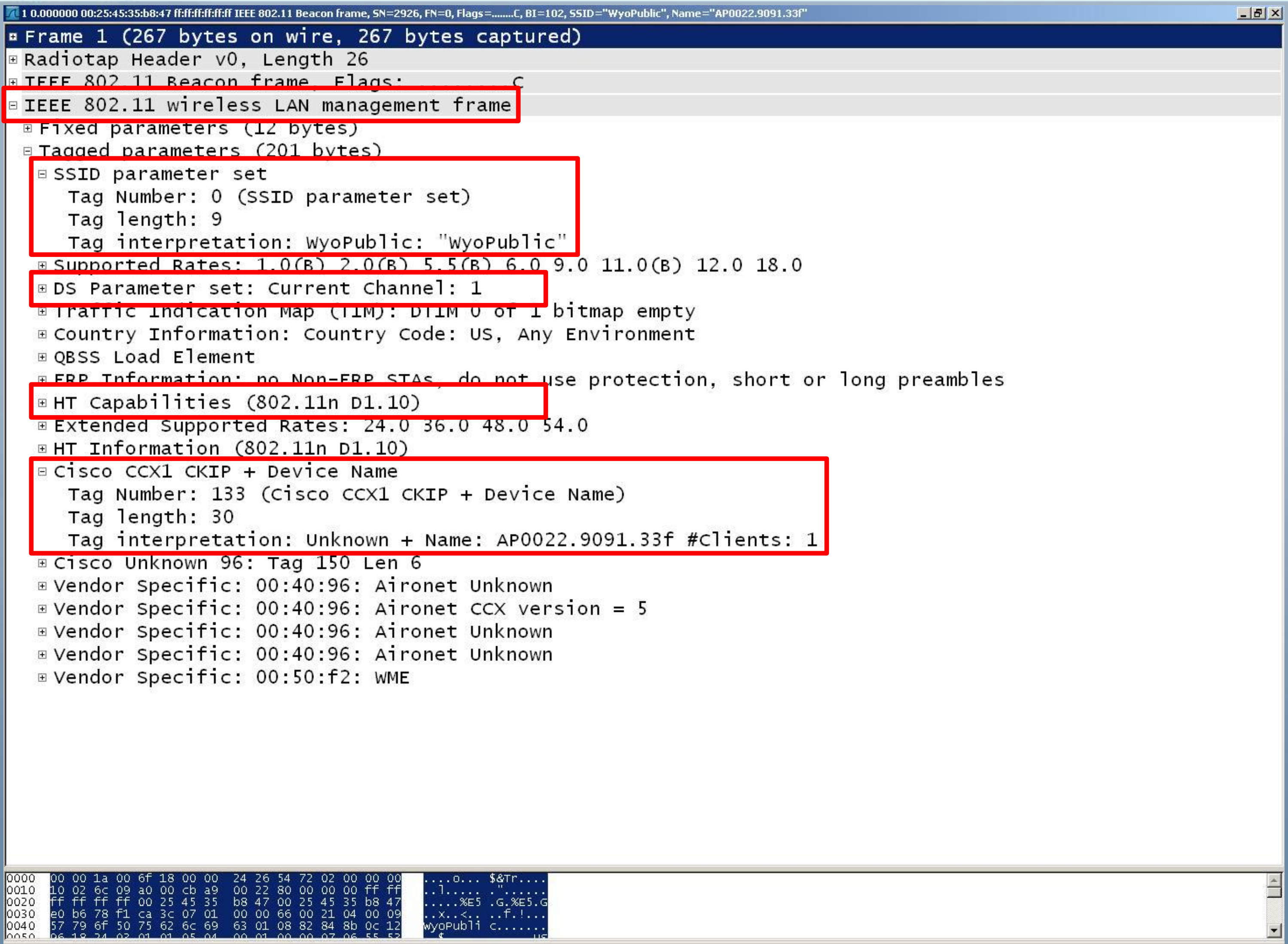


8 0.162603 00:24:01:36:a0:56 ff:ff:ff:ff:ff:ff IEEE 802.11 Beacon frame, SN=908, FN=0, Flags=........C, BI=100, SSID="Emer214A"

```
⊞ Frame 8 (290 bytes on wire, 290 bytes captured)
⊞ Radiotap Header v0, Length 26
⊞ IEEE 802.11 Beacon frame, Flags: ........C
⊟ IEEE 802.11 wireless LAN management frame
  ⊞ Fixed parameters (12 bytes)
  ⊟ Tagged parameters (224 bytes)
    ⊟ SSID parameter set
        Tag Number: 0 (SSID parameter set)
        Tag length: 8
        Tag interpretation: Emer214A: "Emer214A"
    ⊞ Supported Rates: 1.0(B) 2.0(B) 5.5(B) 11.0(B) 6.0 9.0 12.0 18.0
    ⊞ DS Parameter set: Current Channel: 2
    ⊞ Traffic Indication Map (TIM): DTIM 0 of 1 bitmap empty
    ⊞ Country Information: Country Code: US, Any Environment
    ⊞ Power Constraint: Tag 32 Len 1
    ⊞ ERP Information: no Non-ERP STAs, do not use protection, short or long preambles
    ⊟ RSN Information
        Tag Number: 48 (RSN Information)
        Tag length: 24
        Tag interpretation: RSN IE, version 1
        Tag interpretation: Multicast cipher suite: TKIP
        Tag interpretation: # of unicast cipher suites: 2
        Tag interpretation: Unicast cipher suite 1: AES (CCM)
        Tag interpretation: Unicast cipher suite 2: TKIP
        Tag interpretation: # of auth key management suites: 1
        Tag interpretation: auth key management suite 1: PSK
      ⊞ RSN Capabilities: 0x0000
    ⊞ Extended Supported Rates: 24.0 36.0 48.0 54.0
    ⊞ Vendor Specific: 00:50:f2: WME
    ⊞ Vendor Specific: 00:90:4c: HT Capabilities (802.11n D1.10)
    ⊞ HT Capabilities (802.11n D1.10)
    ⊞ Vendor Specific: 00:90:4c: HT Additional Capabilities (802.11n D1.00)
    ⊞ HT Information (802.11n D1.10)
    ⊞ Vendor Specific: 00:03:7f
```

```
0000  00 00 1a 00 6f 18 00 00  4f a1 56 72 02 00 00 00   ....o... O.Vr....
0010  10 02 6c 09 a0 00 b8 a9  00 0f 80 00 00 00 ff ff   ..l..... ........
0020  ff ff ff ff 00 24 01 36  a0 56 00 24 01 36 a0 56   .....$.6 .V.$.6.V
0030  c0 38 80 71 8c 89 01 00  00 00 64 00 31 05 00 08   .8.q.... ..d.1...
0040  45 6d 65 72 32 31 34 41  01 08 82 84 8b 96 0c 12   Emer214A ........
0050  18 24 03 01 02 05 04 00  01 00 00 07 06 55 53 20   .$...... .....US
```

# Public (open) wireless

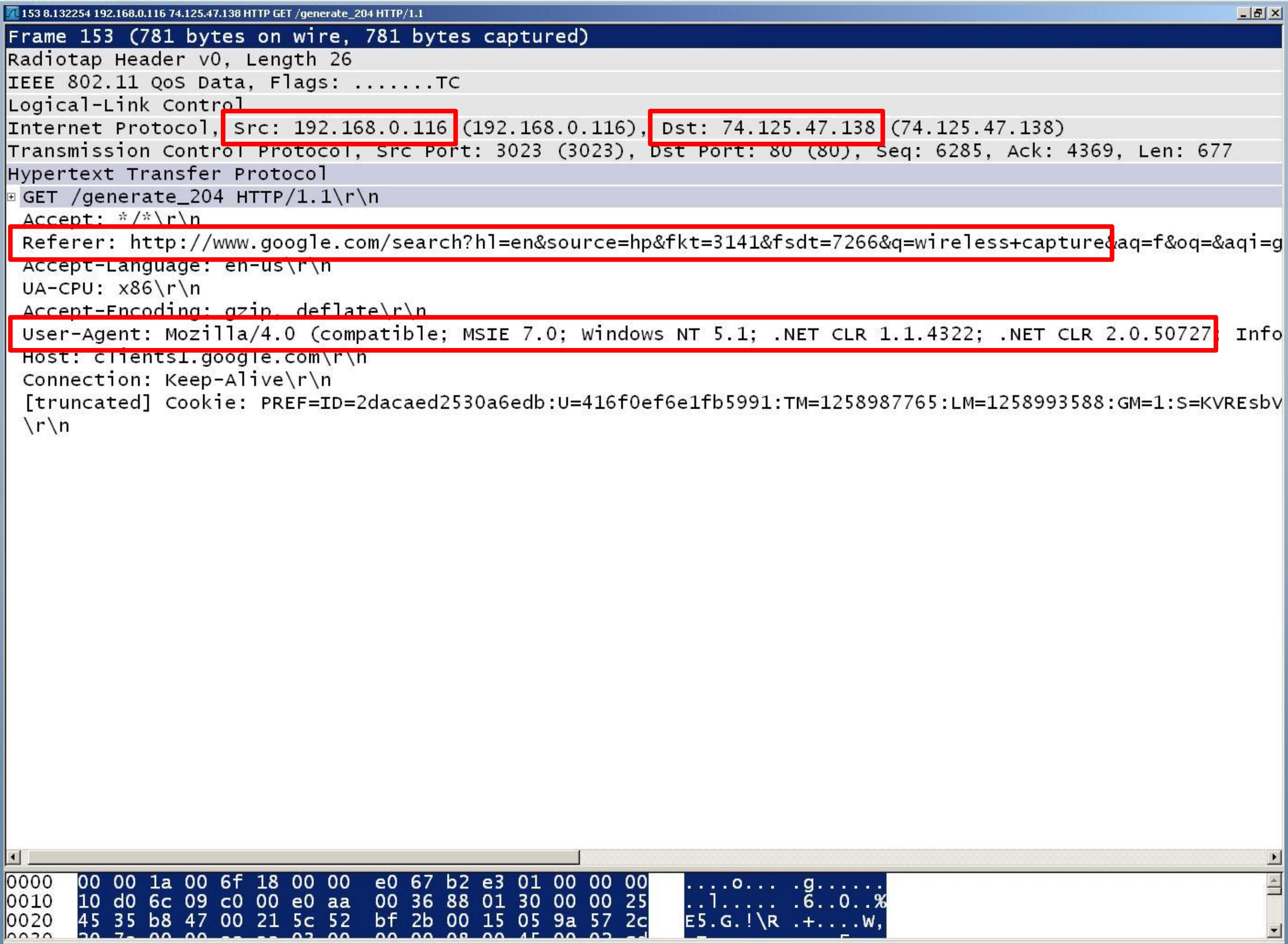


```
1 0.000000 00:25:45:35:b8:47 ff:ff:ff:ff:ff:ff IEEE 802.11 Beacon frame, SN=2926, FN=0, Flags=........C, BI=102, SSID="WyoPublic", Name="AP0022.9091.33f"

⊞ Frame 1 (267 bytes on wire, 267 bytes captured)
⊞ Radiotap Header v0, Length 26
⊞ IEEE 802.11 Beacon frame, Flags: ........C
⊟ IEEE 802.11 wireless LAN management frame
  ⊞ Fixed parameters (12 bytes)
  ⊟ Tagged parameters (201 bytes)
    ⊟ SSID parameter set
        Tag Number: 0 (SSID parameter set)
        Tag length: 9
        Tag interpretation: WyoPublic: "WyoPublic"
    ⊞ Supported Rates: 1.0(B) 2.0(B) 5.5(B) 6.0 9.0 11.0(B) 12.0 18.0
    ⊞ DS Parameter set: Current Channel: 1
    ⊞ Traffic Indication Map (TIM): DTIM 0 of 1 bitmap empty
    ⊞ Country Information: Country Code: US, Any Environment
    ⊞ QBSS Load Element
    ⊞ ERP Information: no Non-ERP STAs, do not use protection, short or long preambles
    ⊞ HT Capabilities (802.11n D1.10)
    ⊞ Extended Supported Rates: 24.0 36.0 48.0 54.0
    ⊞ HT Information (802.11n D1.10)
    ⊟ Cisco CCX1 CKIP + Device Name
        Tag Number: 133 (Cisco CCX1 CKIP + Device Name)
        Tag length: 30
        Tag interpretation: Unknown + Name: AP0022.9091.33f #Clients: 1
    ⊞ Cisco Unknown 96: Tag 150 Len 6
    ⊞ Vendor Specific: 00:40:96: Aironet Unknown
    ⊞ Vendor Specific: 00:40:96: Aironet CCX version = 5
    ⊞ Vendor Specific: 00:40:96: Aironet Unknown
    ⊞ Vendor Specific: 00:40:96: Aironet Unknown
    ⊞ Vendor Specific: 00:50:f2: WME

0000  00 00 1a 00 6f 18 00 00  24 26 54 72 02 00 00 00   ....o... $&Tr....
0010  10 02 6c 09 a0 00 cb a9  00 22 80 00 00 00 ff ff   ..l..... ."......
0020  ff ff ff ff 00 25 45 35  b8 47 00 25 45 35 b8 47   .....%E5 .G.%E5.G
0030  e0 b6 78 f1 ca 3c 07 01  00 00 66 00 21 04 00 09   ..x..<.. ..f.!...
0040  57 79 6f 50 75 62 6c 69  63 01 08 82 84 8b 0c 12   WyoPubli c.......
0050  06 18 24 03 01 01 05 04  00 01 00 00 07 06 55 53   .$...... ......US
```

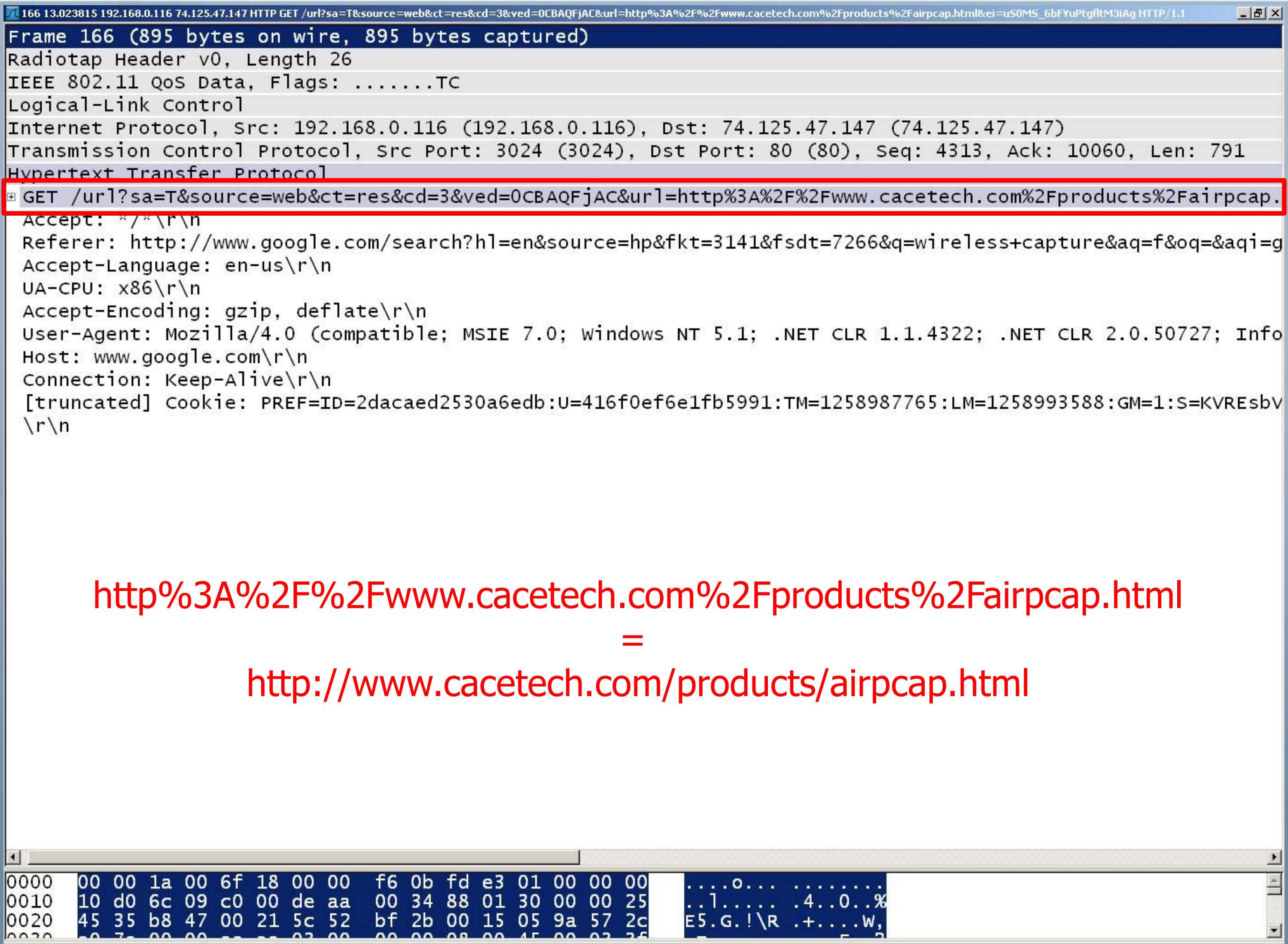
# Public (open) wireless



```
153 8.132254 192.168.0.116 74.125.47.138 HTTP GET /generate_204 HTTP/1.1
Frame 153 (781 bytes on wire, 781 bytes captured)
Radiotap Header v0, Length 26
IEEE 802.11 QoS Data, Flags: .......TC
Logical-Link Control
Internet Protocol, Src: 192.168.0.116 (192.168.0.116), Dst: 74.125.47.138 (74.125.47.138)
Transmission Control Protocol, Src Port: 3023 (3023), Dst Port: 80 (80), Seq: 6285, Ack: 4369, Len: 677
Hypertext Transfer Protocol
⊞ GET /generate_204 HTTP/1.1\r\n
  Accept: */*\r\n
  Referer: http://www.google.com/search?hl=en&source=hp&fkt=3141&fsdt=7266&q=wireless+capture&aq=f&oq=&aqi=g
  Accept-Language: en-us\r\n
  UA-CPU: x86\r\n
  Accept-Encoding: gzip, deflate\r\n
  User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; Info
  Host: clients1.google.com\r\n
  Connection: Keep-Alive\r\n
  [truncated] Cookie: PREF=ID=2dacaed2530a6edb:U=416f0ef6e1fb5991:TM=1258987765:LM=1258993588:GM=1:S=KVREsbV
  \r\n

0000  00 00 1a 00 6f 18 00 00  e0 67 b2 e3 01 00 00 00   ....o... .g......
0010  10 d0 6c 09 c0 00 e0 aa  00 36 88 01 30 00 00 25   ..l..... .6..0..%
0020  45 35 b8 47 00 21 5c 52  bf 2b 00 15 05 9a 57 2c   E5.G.!\R .+....W,
```

# Public (open) wireless



```
166 13.023815 192.168.0.116 74.125.47.147 HTTP GET /url?sa=T&source=web&ct=res&cd=3&ved=0CBAQFjAC&url=http%3A%2F%2Fwww.cacetech.com%2Fproducts%2Fairpcap.html&ei=uS0MS_6bFYuPtgfltM3iAg HTTP/1.1
Frame 166 (895 bytes on wire, 895 bytes captured)
Radiotap Header v0, Length 26
IEEE 802.11 QoS Data, Flags: .......TC
Logical-Link Control
Internet Protocol, Src: 192.168.0.116 (192.168.0.116), Dst: 74.125.47.147 (74.125.47.147)
Transmission Control Protocol, Src Port: 3024 (3024), Dst Port: 80 (80), Seq: 4313, Ack: 10060, Len: 791
Hypertext Transfer Protocol
⊞ GET /url?sa=T&source=web&ct=res&cd=3&ved=0CBAQFjAC&url=http%3A%2F%2Fwww.cacetech.com%2Fproducts%2Fairpcap.
  Accept: */*\r\n
  Referer: http://www.google.com/search?hl=en&source=hp&fkt=3141&fsdt=7266&q=wireless+capture&aq=f&oq=&aqi=g
  Accept-Language: en-us\r\n
  UA-CPU: x86\r\n
  Accept-Encoding: gzip, deflate\r\n
  User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; Info
  Host: www.google.com\r\n
  Connection: Keep-Alive\r\n
  [truncated] Cookie: PREF=ID=2dacaed2530a6edb:U=416f0ef6e1fb5991:TM=1258987765:LM=1258993588:GM=1:S=KVREsbV
  \r\n
```

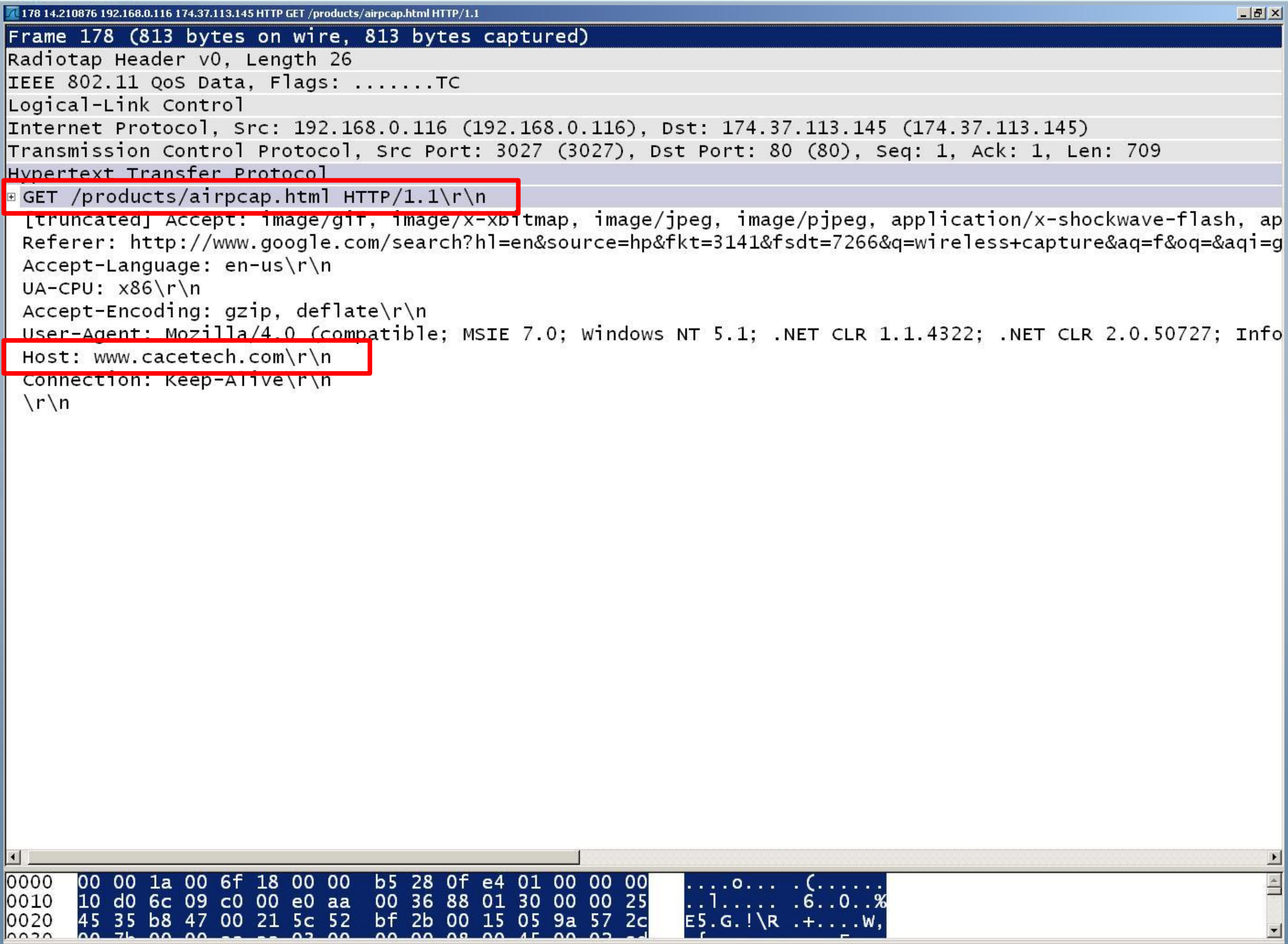
http%3A%2F%2Fwww.cacetech.com%2Fproducts%2Fairpcap.html

=

http://www.cacetech.com/products/airpcap.html

```
0000   00 00 1a 00 6f 18 00 00  f6 0b fd e3 01 00 00 00   ....o... ........
0010   10 d0 6c 09 c0 00 de aa  00 34 88 01 30 00 00 25   ..l..... .4..0..%
0020   45 35 b8 47 00 21 5c 52  bf 2b 00 15 05 9a 57 2c   E5.G.!\R .+....W,
```

# Public (open) wireless



178 14.210876 192.168.0.116 174.37.113.145 HTTP GET /products/airpcap.html HTTP/1.1

```
Frame 178 (813 bytes on wire, 813 bytes captured)
Radiotap Header v0, Length 26
IEEE 802.11 QoS Data, Flags: .......TC
Logical-Link Control
Internet Protocol, Src: 192.168.0.116 (192.168.0.116), Dst: 174.37.113.145 (174.37.113.145)
Transmission Control Protocol, Src Port: 3027 (3027), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 709
Hypertext Transfer Protocol
⊞ GET /products/airpcap.html HTTP/1.1\r\n
  [truncated] Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, ap
  Referer: http://www.google.com/search?hl=en&source=hp&fkt=3141&fsdt=7266&q=wireless+capture&aq=f&oq=&aqi=g
  Accept-Language: en-us\r\n
  UA-CPU: x86\r\n
  Accept-Encoding: gzip, deflate\r\n
  User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; Info
  Host: www.cacetech.com\r\n
  Connection: Keep-Alive\r\n
  \r\n
```

```
0000  00 00 1a 00 6f 18 00 00  b5 28 0f e4 01 00 00 00   ....o... .(......
0010  10 d0 6c 09 c0 00 e0 aa  00 36 88 01 30 00 00 25   ..l..... .6..0..%
0020  45 35 b8 47 00 21 5c 52  bf 2b 00 15 05 9a 57 2c   E5.G.!\R .+....W,
```

# Social networks

Created with sharing in mind NOT privacy or security

- Use your “Friends List”
- Remove yourself from search results
- Make your contact information private
- Keep your friendships private

# Data backups

- Easy and inexpensive to perform
- Difficult and costly to replace

- 64 GB of storage $135

- 250 GB of storage $100
- 1 TB of storage as low as $90

# Data backups

- Lots of applications on the market
- Consider a full disk image to backing up data
- Label your backup media or images
  - Date of backup/image
  - What’s on it
- Store backups in a safe location
  - Fire proof box
  - Someone else's house

# QUESTIONS